

IN THE UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TENNESSEE

STATE OF TENNESSEE

COUNTY OF SHELBY

Case No. 22-SW-241

**ATTACHMENT C**  
**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, **Matthew Upshaw**, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the FBI and have been so employed since September 26, 2021. I am currently assigned to a squad that investigates matters involving the sexual exploitation of children, human trafficking, and child sexual abuse material (CSAM). I have participated in multiple search warrants leading to the seizure of items having evidentiary value. Since joining the FBI I have received training on the investigation and prosecution of criminal cases. I have gained experience through training in seminars, classes, and everyday work related to conducting these types of investigations.

2. I make this affidavit in support of an application for a search warrant for information associated with certain Microsoft Corporation accounts associated with the identifier, “**gman921@live.com**” (Outlook), that are stored at premises controlled by Microsoft Corporation (“Microsoft”), which is an electronic communications and remote computing service provider headquartered at 1 Microsoft Way, Redmond, Washington 98052. The information to be searched is described in the following paragraphs and in **Attachment A**. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Microsoft to disclose to the government copies of the information

(including the content of communications) further described in Section I of **Attachment B**. Upon receipt of the information described in Section I of **Attachment B**, government-authorized persons will review that information to locate the items described in Section II of **Attachment B**.

3. Based on my training and experience, and facts as set forth in this affidavit, there is probable cause to believe that items which constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C Section 2251(a) (production/attempted production of child pornography) and 18 U.S.C. Section 1470 (transfer of obscene material to a minor) are contained within information associated within the Microsoft identifier “**gman921@live.com**” (hereby by known as the “Account”), which are described more fully in **Attachment A**.

4. The following information was obtained through the assistance of other law enforcement agents and agencies, including their reports, and through other sources specifically named in this affidavit. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, U.S.C. Section 2251(a) and Title 18, U.S.C. Section 1470 will be located at the premises described in **Attachment A**, and consist of or be contained in the items listed in **Attachment B**, both of which are incorporated by reference as if fully set forth herein.

#### APPLICABLE STATUTES

5. Title 18, United States Code, Section 2251(a) makes it a federal offense for anyone to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in sexually

explicit conduct as defined in Title 18, United States Code, Section 2256(2)(A), for the purpose of producing a visual depiction of such conduct, or attempts to do so.

6. 18 U.S.C. §§ 1470 makes it a federal offense for anyone, using a means of interstate or foreign commerce, to knowingly transfer obscene material to another individual who has not attained the age of 16 years, or attempts to do so.

### **DEFINITIONS**

7. The following definitions apply to this affidavit and **Attachment B**:

a. The term "minor," as used herein, is defined pursuant to Title 18 U.S.C. §2256(1) as "any person under the age of eighteen years."

b. As it is used in 18 U.S.C. § 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2)(A), and includes sexual intercourse of any kind, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; and the lascivious exhibition of genital or pubic area.

c. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography" is defined in 18 U.S.C. § 2256(8), and includes any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in "sexually explicit conduct".

d. The term "sexually explicit conduct" has the same meaning in § 2252A as in §2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B), to include (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

e. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

f. The term "visual depiction," as used herein, is defined pursuant to Title 18 U.S.C. § 2256(5) to include "undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."

g. The term "producing," as used herein, is defined pursuant to Title 18 U.S.C. §2256(3) to include "producing, directing, manufacturing, issuing, publishing, or advertising".

h. The term "computer" is defined in Title 18 U.S.C. § 1030(e)(I) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

i. The term "Internet", as used herein, refers to the global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices' communication with each other are in the same state.

j. The term "Internet Protocol address" (IP), as used herein, refers to a unique number used by an Internet accessible device, which is used to access the Internet. IP addresses are assigned by "Internet Service Providers" or "ISPs", which are commercial organizations that provide a range of functions for their customers including access to the Internet, web hosting, email, and remote storage.

k. The term "electronic communication service" is defined in Title 18 U.S.C. §2510(15) as any service which provides to users thereof the ability to send or receive wire or "electronic communications", which refer to any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce.

l. The term "electronic storage" as defined in Title 18 U.S.C. § 2510 (17) means any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and any storage of such communication by an "electronic communication service" for purposes of backup protection of such communication.

m. The term "electronic device", as used herein, is defined as any portable, electrical powered device capable of sending or receiving a wireless signal; storing, sending, or retrieving electronic data; or having computing capability.

n. The term "chat/chat group", as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally shorter, resembling an oral conversation, and are distinguished from other text-based online communications such as Internet forums and email.

**CHARACTERISTICS OF INDIVIDUALS WHO ACCESS WITH INTENT TO VIEW, PRODUCE, RECEIVE AND POSSESS CHILD PORNOGRAPHY**

8. Based on my knowledge, training, and experience, and the experience and training of other law enforcement officers in child exploitation investigations with whom I have had discussions, there are certain characteristics that are prevalent among individuals who are involved in the production, receipt, and possession of child pornography:

a. The majority of individuals who produce and collect child pornography are persons who have a sexual attraction to children, and may engage in the sexual abuse of children or exchange and collect child pornography and child erotica to receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.

b. Individuals who produce and collect child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videos, drawings or other visual media. Not only do collectors oftentimes use these materials for their own sexual arousal and gratification, but they also may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. The majority of individuals who collect and produce child pornography often seek out like-minded individuals, either in person or via the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance, and support. Individuals who collect and produce child pornography often correspond with and/or meet others to share information and materials and often maintain lists of names,

usernames, addresses, emails, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography and child sexual abuse.

d. Persons committing these criminal acts, more likely than not, almost always possess and maintain their hard copy and/or digital medium collections of child pornographic and child erotica material in a secure and private environment. Due to the psychological support their collections provide, such individuals find comfort and justification for their illicit behavior and desires and rarely destroy such materials. As such, these collections are often maintained for several years and are kept close by, usually in a location that is mobile and/or easily accessible to the individual.

e. In some cases, people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on computers or digital devices for months or even years after any downloaded files have been deleted.

f. Collectors of child pornography frequently prefer not to be without their child pornography for any prolonged time period, and more likely than not may go to great lengths to conceal and protect their collection of illicit materials from discovery, theft, and damage. This behavior has been documented by law enforcement officers involved in child exploitation and pornography investigations worldwide.

#### **BACKGROUND REGARDING ELECTRONIC DEVICES AND THE INTERNET**

9. Based on my knowledge, training, and experience, and conversations I've had with other law enforcement officers investigating crimes involving the online sexual exploitation of children, I know the following:

7 MBU  
8/29/22



a. Computing technology has not only changed the way in which children are exploited in the production, collection, storage and distribution of child pornography and child erotica materials, but also in how individuals who sexual exploit children interact with one another.

b. Advancements in technology, to include accessibility to the Internet, have made it easier for individuals to communicate, produce, store, and distribute child pornography and child erotica in a manner that is inexpensive and relatively anonymous. Internet connected devices, such as computers and smart phones, provide collectors of child pornography with different venues for obtaining, viewing, and trading child pornography and child erotica.

c. In particular, a computer is ideal for storing large quantities of digital media and is an ideal repository for child pornography. Communications by way of computer can be saved and stored intentionally or unintentionally. In addition to electronic communications, a computer user's activities (such as Internet browsing or utilization of peer to peer software) leave traces that can be recovered via a forensic examination.

d. Individuals who collect child pornography may also utilize various forms of portable electronic storage media that, more likely than not, are used on Internet connected devices and/or other forms of electronic storage media, such as external hard drives, flash drives, and USB thumb drives, which can store hundreds of thousands of digital media. Portable electronic storage media are typically utilized by collectors of child pornography due to increased storage capacity, ease of concealment, and the ability to encrypt illicit materials.

e. Cell phones and "smart phones" function similarly to computers and have been used to send, receive, store, and produce media depicting child pornography, as well as engage in voice, email, text, and real time chat conversations with minors and others. Mobile devices can



also contain secure digital (SD) cards and/or subscriber identity module (SIM) cards which can be used to store data such as pictures, videos, text messages, contact lists, call logs and other data.

f. Individuals who produce and collect child pornography, more likely than not, use online resources such as companies that provide electronic communication and "cloud based" services to retrieve and store child pornography and child erotica. Electronic communication service providers, such as Gmail, Apple, Microsoft, and Dropbox among others, can be utilized for online storage which can be accessed from any Internet connected device, such as a computer or mobile phone. Even in cases when online storage is used, evidence of child pornography can be found on the user's electronic devices in most cases.

### INVESTIGATION

10. On June 21, 2022, a trained FBI Online Covert Employee (OCE), who was posing as a 14-year-old female from Memphis named Natasha, was contacted by an unknown individual who responded to a post via Whisper, an anonymous social networking application. The Whisper post stated "I'm really 18 minus 4." The unknown individual, with the display name of "Undecided\_Bronze," described himself as a 21-year-old male from Akron. The two exchanged pictures after "Undecided\_Bronze" was advised Natasha was a 14-year-old female. The unknown individual in the picture appeared to be a white male with yellow highlights in his hair. On his face were a pair of black rimmed glasses and facial piercing's in his nose and mouth.

11. "Undecided\_Bronze" asked if Natasha had a Snapchat account and provided his username to her as "xxamn3siaxx", hereby referenced as the Snapchat Account. Natasha added the unknown individual on June 21, 2022, where he identified himself as "Geo." The unidentified individual sent Natasha a live Snap, which your affiant knows is generally when a picture is taken

within the application and not a picture that was selected from a user's camera roll – meaning it was a new picture taken in the moment, with the text “I told you I’m real.” The male in the image looked visually identical to the male in the image sent by “Undecided\_Bronze” on the Whisper app. The unknown individual then demanded Natasha prove she was also real.

12. After confirming she was a 14-year-old female, they engaged in a brief discussion about their reasons for being on Whisper. The unknown individual told Natasha “A lot of guys are looking for nudes on whisper.” Natasha asked the unknown individual if he was looking for nudes from her. The unknown individual responded “I feel kinda wrong for asking. I don’t want to make you uncomfy.” Natasha further inquired if the unknown individual felt 14 was too young. The unknown individual responded by asking Natasha about guys her own age. Natasha told the unknown individual guys her own age were too immature. The unknown individual responded “Yeah. Go ahead baby (wink emoji)” and told Natasha to “...send a pic of your boobs, butt and pussy”, which is considered child sexual abuse material (CSAM).

13. On June 22, 2022, the unknown individual sent Natasha a Snap of what appeared to be of a nude male penis in an aroused state. Natasha asked the unknown individual if the image was of his penis. The unknown individual stated “It sure was. No way i could fake a live snap. Do you have any more pics for me?” During their conversation, the unknown individual sent two Snaps that were sexually explicit. One appeared to be of a nude male penis in an aroused state and the other appeared to be a video of a nude male masturbating.

14. A subpoena was submitted to Snap, Inc. seeking subscriber information associated with the Snapchat Account. On or around June 22, 2022, Snap, Inc. provided the following subscriber information and IP address logs:

<b>Identifier</b>	xxamn3siaxx
<b>Display Name</b>	Geo .
<b>Phone Number</b>	+13309797251
<b>Login IP Address</b>	24.33.88.47

15. An open source “who-is” search was conducted for IP address 24.33.88.47, which was provided by Snap, Inc. as being used to access the Snapchat Account during the timeframe of the alleged criminal activity, revealed that the IP address is registered to Charter Communications for assignment to their Internet customers in Akron, Ohio.

16. A subpoena was submitted to Charter Communications for any and all subscriber information associated with IP address 24.33.88.47 on June 2, 2022, at 6:10 UTC. On June 28, 2022, Charter Communications provided subscriber information which identified the subscriber as Michelle Shamrock and the service address of IP address 24.33.88.47 as being located at 1362 Neptune Ave, Akron, OH 44301.

17. A subpoena was submitted to Verizon Wireless seeking any and all subscriber information associated with phone number 330-979-7251, which was provided by Snap, Inc. as being used to register the Snapchat Account. On July 5, 2022, Verizon Wireless identified the subscriber as Geovanni Flask located at residential address 1362 Neptune Ave, Akron, OH 44301. Verizon Wireless further identified a Samsung Galaxy Z Fold3 as being registered to the phone number.

18. Open source research identified a potential suspect as Geovanni Paul Flask. A search of the Ohio driver license database showed an image from Flask’s Ohio driver’s license, which looked visually similar to the individual that sent a photo of himself via Whisper and

Snapchat, and also listed his residential address as 1362 Neptune Ave, Akron, OH 44301. Further research revealed Flask possibly lived with his mother, Michelle Shamrock and his 8-year-old daughter.

19. On July 14, 2022, a federal search warrant was executed in the Northern District of Ohio for the person of Flask at his residence. Flask was present and agreed to speak with FBI agents. During his voluntary interview with FBI agents, Flask admitted talking to underage girls on different social networking apps to include Whisper, Kik and Snapchat. Flask stated the conversations involved pictures being sent only if he sent a picture. Flask admitted he knew what he was doing was wrong as he knew the girls were minors. Flask advised he only used his mobile phone to communicate with underage girls, which he identified as a Samsung Z-Fold 3 with telephone number 330-979-7251. Flask acknowledged he used the Kik username "clubgeo921" and the Snapchat Account "xxamn3siaxx". According to Flask, people believed Snapchat was more anonymous because content was deleted. Flask also advised he used the email accounts gman921@live.com and geovanni.flask921@gmail.com.

20. A Samsung Galaxy Z Fold3 was seized during the execution of the federal search warrant and an examination was conducted on the device, which belonged to Flask. FBI Agents located Snapchat which was logged in on the device with the account "xxamn3siaxx". The account used by Natasha was observed to have been blocked by Flask. FBI agents located Whisper which was logged in on the device and contained the conversation between Flask and Natasha that occurred on June 21, 2022.

21. FBI agents also observed conversations between Flask and unknown individuals via the Whisper app. In many of the conversations, Flask requested nude photos from unknown individuals that appeared to be female. In particular, an unknown individual agreed to provide

nude photos for \$15 via CashApp and asked for Flask Snapchat username, which he provided as “xxamn3siaxx”. In another conversation, Flask responded to a post via Whisper where an unknown individual with the display name “Spent\_Yaddah” asked Flask if he was interested in “Children Porn”. Flask confirmed that he was interested and responded “Preview?”. The unknown individual advised they charged \$70 for the Dropbox link and sent an image of what appeared to be a Dropbox link of a folder labeled “wendy”. The thumbnail images appeared to depict prepubescent minors engaged in sexually explicit activity consistent with child pornography / CSAM.

22. FBI agents also observed sexually explicit images of young women that appeared to be between the ages of 14 and 18 saved in archived emails on a Microsoft Office account associated with the email address **gman921@live.com**. The emails appeared to have been sent from the Account to the Account and contained subject lines with no subjects or else appeared to be titled with app names e.g., “Kik1.” For example, within one of the emails was a MP4 type video saved as “snapchat-2004458519.mp4.” In the body of the email were identifiable nude images of females that appeared between the ages of 14 and 18 years of age.

23. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 1470 and 2251(a) have been committed, and evidence, instrumentalities and fruits of those violations are located at the PREMISES further described in **Attachments A and B** of this affidavit.

24. I respectfully submit there is probable cause to believe that the Account to be searched still contains the items to be seized, as set forth in **Attachment B**. Based on my training, my experience and this investigation, I know that because of constantly expanding capacities for online accounts, people tend to keep emails and other information such as attached files in their

accounts for long periods of time. In fact, online service providers expressly encourage their subscribers to retain their emails and other information by offering increasingly larger email boxes and other services. That said, if a user deletes information, the information can still remain on the service provider's servers for some time. This is because a service provider, such as Microsoft, often maintains backup copies on servers globally to ensure account holders maintain access to their data.

### **INFORMATION REGARDING MICROSOFT**<sup>1</sup>

25. Based on my knowledge and experience, I know that Microsoft Corporation ("Microsoft") is a technology corporation headquartered at 1 Microsoft Way, Redmond, WA 98052. Microsoft provides a variety of products and services which range from software, such as operating systems and software development tools, to hardware, such as personal computers, tablets and gaming consoles. Microsoft also provides various services, which can be accessed via a Microsoft account (MSA). MSA is a single sign-on user account that allows customers to access Microsoft services, application software, and devices using Microsoft operating systems (i.e. Microsoft Windows, Windows Phones, and Xbox consoles). Subscribers to Microsoft services provide basic subscriber information to Microsoft and may access their accounts on servers maintained and/or owned by Microsoft from any computer with Internet access.

26. In particular, your affiant is aware that Outlook is an email service provided by Microsoft which is available free of charge to Internet users. Microsoft maintains electronic records to include account access information, email transaction information, and account

---

<sup>1</sup> The information in this section is based on information published by Microsoft Corporation. via their Law Enforcement Guide and on their website.

application information. Your affiant is also aware that any email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by Microsoft. If the message is not deleted by the subscriber, it is possible that the message can remain on Microsoft's servers indefinitely.

27. I know due to the multitude of services provided, additional information is captured by Microsoft in connection with the use of a Microsoft account access to certain services. For example, Outlook retains IP log data which is captured at the time of the user login to the email service. Microsoft allows users to store files, including emails, images and video files on servers maintained or owned by Microsoft. Emails and image files stored on a Microsoft server by a subscriber may not necessarily be located in the subscriber's personal electronic device. The subscriber may store emails and other files on the Microsoft server for which there is insufficient storage space in the subscriber's electronic device or which the subscriber does not wish to maintain on their devices.

28. In my training and experience, evidence of who was using a Microsoft account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In this particular case, your affiant is aware that images of nude females which appeared to be between the ages of 14 and 18 were observed in the Account and that retrieval of Microsoft data may identify additional victims of child online exploitation.



### JURISDICTION

29. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### CONCLUSION

30. Based on the forgoing factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 1470 and 2251(a) have been committed, and evidence of those violations can be found in the Account, stored at premises controlled by Microsoft. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of items described in **Attachment B** of this Affidavit.

31. This application seeks a warrant to search all responsive records and information under the control of Microsoft, a provider subject to the jurisdiction of this court, regardless of where Microsoft has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft’s possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

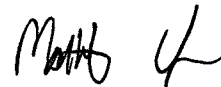
32. Your affiant is aware that many providers of digital services, such as Microsoft., have staff members who work shifts other than traditional business hours. Such staff members may at times be responsible for compiling materials responsive to search warrants. Therefore, your

affiant requests that this warrant be executable at any time of the day or night, as that may be more convenient for the responding party.

33. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

34. In consideration of the foregoing, your affiant respectfully requests that this Court issue a search warrant for the search of the Microsoft Account, more specifically described in **Attachment A** which is incorporated by reference as if fully set forth herein, authorizing the seizure and search of the items described in **Attachment B**, incorporated herein.

AND FURTHER, AFFIANT SAITH NOT.



Matthew Upshaw - AFFIANT  
Special Agent,  
Federal Bureau of Investigation.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 41 by telephone, this 29th day of August, 2022.

  
HON. ANNIE T. CHRISTOFF  
United States Magistrate Judge